UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/712,396	11/14/2003	Steven Y. Zhou	8971.0005	6846

22852 7590 03/30/2010

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
DAFTUAR, SAKET K	

ART UNIT	PAPER NUMBER
2451	

MAIL DATE	DELIVERY MODE
03/30/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/712,396	ZHOU, STEVEN Y.	
	Examiner	Art Unit	
	SAKET K. DAFTUAR	2451	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 January 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,10-12,21,22,24-33,37-40,44 and 45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7, 10-12, 21-22, 24-33, 37-40 and 44-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Response to Amendment

1. This office action is responsive to the amendment filed on January 19th, 2010. Claims 1-7, 10-12, 21-22, 24-33, 37-40 and 44-45 are presented for the further examination. Applicant has cancelled claims 8, 9, 13-15, 18-20, 23, 34-36, and 41-43 by this amendment.

Interview Remarks

2. Examiner has contacted applicant assigned representative on March 19th, 2010 with examiner amendment proposal to amend all independent claims to include "determine quadrant value" based on Multidimensional space or tuple space with respect to "hash function and modulo division "and cancel claims 1, 3-7, 27, 30 and 45. However, as March 25th, 2010, no further agreement and authorization has been received from the applicant assigned representative.

Response to Arguments

3. Applicant's arguments with respect to claims 1-7, 10-12, 21-22, 24-33, 37-40 and 44-45 have been considered but they are not persuasive.

a. As per arguments filed on January 19th, 2010, applicant continues to argue to the substance that cited prior arts failed to teach or suggest each and every limitation of claimed subject matter as claimed in claims 1, 10, and 24. Other claims are respectively parallel to claims 1, 10 and 24.

In response to applicant argument a), examiner earlier made a comment that claims would be allowable if amended to include "multidimensional address space is determined based on hash function and division modulo.." However, applicant failed to amend the claims accordingly. Applicant continues to argue that one of the cited prior art Bosley fails to teach or disclose or suggeste each and every limitation in the claims as a whole and continues to argue that the secondary references fail to cure the deficiencies of Bosley but merely provides any argument with respect to claimed subject matter. As such examiner respectfully reminds applicant that applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Bosley is directed to a hypercube model where hash key is generated for each servers and describes the location or address of each server at particular given time (see column 6, line 30 – column 7, line 50 below) .

> "In our randomized hypercube model, each of the n servers obtains a unique 160-bit hash key in the interval [0,1) using the SHA1 hash function. (SHA1 was chosen for its cryptographic properties of collision resistance; it is easy to use a different hash function instead if desired, even one with fewer bits. The system needs to be collision resistant, thus the number of bits should be at least twice the log of the number of objects in the system in order to have low probability of this occurring, and it should be cryptographically resistant so that files cannot be manufactured which match existing files, that is, it is not easy to generate x such that h(x)=h(y) for a given y. For a billion objects, this is about at least 60 bits; for a trillion it is 80 bits. Therefore 160 is more than necessary.) This hash key (the node ID) describes the server's "location" in the interval. Each server is assigned a list of contacts (a contact is a server that the server "knows" exists) with which it communicates directly."

"FIG. 4 uses the same method of representing a hypercube shown in FIG. 3, except that it provides three different views of this hypercube representing different subsets of its dimensions. The portion of FIG. 4 encircled within the dotted line 400 corresponds to that shown in FIG. 3, which illustrates the first nine dimensions of the hypercube. The portion of FIG. 4 shown within the dotted line 402 is a blowup of what appears to be an individual node 201a within the dotted circle 400. This blowup shows the next nine dimensions 9 through 17, for the hypercube. It should be appreciated that each individual corner of each of the small rectangles 302 shown in FIG. 3 and FIG. 4 actually correspond to a hierarchy of cubes defined by the smaller dimensions of the hypercube representation. It should be appreciated that each actual node in this higher dimensional hypercube is connected by all dimensions of the hypercube to any other node which varies from it only by the value of the bit represented by that given dimension.

The 160 bit hash value used in the current embodiment of the Skyris network represents a binary number large enough to represent over a trillion trillion trillion possible values. Thus even if a given Skyris network has a large number of nodes, only a very small percent of the possible values that can be defined by such a large binary value will actually have a node associated with them. For this reason if the 160 bit hash value is represented as a hypercube, that hypercube will be largely empty. This is illustrated by FIG. 4 in which the hypercube formed by a large set of nodes, such as a billion nodes would look quite full when looking at only the nine highest order bits of the hash address space, because in the hierarchical cubic representation shown in that figure each corner of one of the smallest cubes 302 shown in the portion of the figure encircled by the dotted lines 400 would tend to have some value associated with them, since each such corner would represent 1/512 of the entire address space, and would be almost certain to have some nodes fall within that portion of the total address space. "

Bosley is directed to a multidimensional address space in computer Network whereas Zenchelsky is directed to a method for peer-level access control on networks that carry packet of information, each packet having a 5-tuple having a source and destination address. (see abstract below) and teaches firewall nodes for processing such packet or packets in network.

"system and method for providing peer-level access control on networks that carry packets of information, each packet having a 5-tuple having a source and destination address, a source and destination port, and a protocol identifier. The local rule base of a peer is dynamically loaded into a filter when the peer is

authenticated, and ejected when the peer is loses authentication. The local rule base is efficiently searched through the use of hash tables wherein a hashed peer network address serves as a pointer the peer's local rules. Each rule comprises a 5-tuple and an action. The action of a rule is carried out on a packet when the 5-tuple of the rule corresponds to the 5-tuple of the packet."

"A typical application of a firewall is shown in FIG. 2. A corporate network 20 may wish to provide access to Internet hosts 21 to its subscribers, but may wish to limit the access that the Internet hosts 21 have to the corporate network 20, which may contain trade secrets and proprietary information. The corporate network 20 would develop a security policy implemented by a firewall 22 placed at the interface between the corporate network 20 and the Internet hosts 21. The firewall 22 comprises a filter 23 that would PASS or DROP packets from Internet hosts 21 to corporate network subscribers 20 and vice versa based upon the packets' source and destination addresses. The firewall is said to belong to the corporate network, and enforces rules that "protect" hosts within the corporate network that have IP addresses. Such hosts are said to be "behind" the corporate network firewall." (see column 2, lines 52-67)

In addition, other than processing packets through firewall nodes, examiner considers Zenchelsky also teaches a method for processing such tuple packet using hash table (see figures 8a – 9, see column 8, line 7-46 below)

" FIG. 8d shows the method by which the hash tables are searched in accordance with the present invention. FIG. 8d represents a detailed view of the box "Check Local Rule Base" 713 in FIG. 7b.

In accordance with the present invention, if there was no corresponding rule found in the global pre-rule base 711 (FIG. 7b), then the local-in hash table is efficiently searched for a rule that corresponds to the packet 841. If a corresponding rule is found and the action is DROP, the packet is dropped 842. If the action is PASS or there is no corresponding rule, the peer-out hash table is checked 843. If a corresponding rule in the hash-out table is found and the action is DROP, the packet is dropped 844. If the action is PASS or there is no corresponding rule, and if at least one of the hash tables contained a corresponding rule, the packet is passed 845. If there were no corresponding rules in either hash table 846, then the post-rule base is checked 715 as shown in FIG. 7b.

Were it not for the peer-in and peer-out hash tables, the rules would have to be searched far less efficiently by searching the entire rule base for rule identifiers (e.g., 5-tuples) that match the packet identifier (e.g., 5-tuple.) The part of the rule that identifies the packet to which the rule applies (the rule identifier) is also called the rule "key." Using hash tables eliminates the need to search the

keys of all rules, pointing instead to the relevant subset of possibly applicable rules through a speedier search. Thus, the scope and computational time needed to carry out the search is substantially and advantageously reduced, reducing the delay in packet transit time caused by the interposition of a filter between the packet source and destination.

As shown in FIG. 9, a peer is first authenticated 91 in accordance with the present invention. Upon authentication, the peer's local rule base is loaded into the filter 92. A hash function is carried out on the peer's network address 93, and the filter's peer-in and peer-out hash tables are updated 94 with pointers to the peer's peer-in and peer-out rules. When the peer is no longer authenticated 95, the peer's local rules are ejected from the filter local rule base 96, and the pointers to the peer's peer-in and peer-out rules are ejected from filter's peer-in and peer-out hash tables 97. "

As such examiner considers the following combination of Bosley, Zenchelsky and Bommareddy, where examiner believes the cited combination of prior arts read on the claimed subject matter. Bosley discloses determining, by the first processing unit (see Figure 1, column 5, lines 11-21), whether the address of the received packet is within space assigned or multi-dimensional space (see figure 2, column 6, line 30- column 7, line 30) to the first processing unit based on a quadrant identifier value [hash value based on number of bit of that represented as hypercube, see figures 2-6, column 6, line 30- column 7, line 50, see column 9, lines 4-24 for the address space corresponds to range of address] assigned to the first processing unit, wherein the space assigned to each of the plurality of processing units is different, and wherein the quadrant identifier is determined using a hash function (see figures 2-6 for quadrant identifier and hash value based on number of bit of that represented as hypercube, column 6, line 30- column 7, line 50, see column 9, lines 4-24); determining that the address is within the space assigned to the first processing unit (Routing, see Figure1 , column 5, lines 3-11); determining, when the address of the received packet is not

within the space assigned to the first processing unit (see figures 2-6, column 6, line 30-column 7, line 50, see column 9, lines 4-24 for the address space corresponds to range of address).

However, Bosley is silent about firewall node for processing a packet based on modified address wherein one of the firewall node is selected from the cluster of firewall nodes within a single network.

Zenchelsky teaches one of the firewall nodes for processing a packet (see Abstract, figure 2, column 2, lines 52-67, column 3,lines 21-40);receiving and reading, the received packet (see Abstract, figure 2-3, column 2, lines 52-67, column 3,lines 21-40);a modified address based on the N-tuple space assigned to the first processing unit, such that the modified address does not conflict with addresses assigned by any of the other plurality of processing units and sending the packet based on the modified N-tuple address (see Abstract, figures 5a-5b, column 2, lines 52-67, column 3,lines 21-67, for assigning different IP address from IP pool and/or updating the user IP address each time user access authenticated, see column 8, lines 1-36 and figure 8A -8C for packet transmission based on peer-in / peer- out hash table based on rule identifier).

Bommareddy teaches a firewall cluster within the single network (see figures 1, 4, and 8, column 1, line 66 – column 2, line 60, column 3, line 1 – column 4, line 58, column 6, line 13 – column 8, line 45, column 9, line 5 - column 10, line 67) and processing the set of data packet from first packet from first address to second address wherein the second address being within a range of addresses assigned by firewall cluster ((see figures 1, 4, and 8, column 1, line 66 – column 2, line 60, column 3,

line 1 – column 4, line 58, column 6, line 13 – column 8, line 45, column 9, line 5 - column 10, line 67, column 11, lines 9-65, column, column 15, line 40 – column 18, line 36)).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the teachings of Bosley, Zenchelsky and Bommareddy to provide a enhanced packet switched data handling method to a high speed network device securely switching data between the high speed network devices communicating behind the firewall clustering system using a enhanced hash function and arithmetic operations whereas the firewall cluster system being configured to operate in manner that creates or configures a firewall cluster on both internal and external network flow controllers to monitor the health of firewalls by probing firewall data packets through both internal and external firewalls whereas the flow controllers distribute traffic based on the source and destination IP addresses of a packet and ensuring that all IP-based protocols are supported and within the range of IP based protocols and repeating the same method steps until all data packets has been processed or securely transmitted to the destination port.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-7, 10-12, 21-22, 24-33, 37-40 and 44-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bosley et al US Patent Number 7,054,867 (hereinafter Bosley), Zenchelsky et al US Patent Number 6,233,686 B1 (hereinafter Zenchelsky) and further in view of Bommareddy et al US Patent Number 6,880,089 (hereinafter Bommareddy).

As per claim 10, Bosley discloses determining, by the first processing unit (see Figure 1, column 5, lines 11-21), whether the address of the received packet is within space assigned or multi-dimensional space (see figure 2, column 6, line 30- column 7, line 30) to the first processing unit based on a quadrant identifier value [hash value based on number of bit of that represented as hypercube, see figures 2-6, column 6, line 30- column 7, line 50, see column 9, lines 4-24 for the address space corresponds to range of address] assigned to the first processing unit, wherein the space assigned to each of the plurality of processing units is different, and wherein the quadrant identifier is determined using a hash function (see figures 2-6 for quadrant identifier and hash value based on number of bit of that represented as hypercube, column 6, line 30- column 7, line 50, see column 9, lines 4-24); determining that the address is within the space assigned to the first processing unit (Routing, see Figure1 , column 5, lines 3-11); determining, when the address of the received packet is not within the space assigned to the first processing unit (see figures 2-6, column 6, line 30- column 7, line 50, see column 9, lines 4-24 for the address space corresponds to range of address).

However, Bosley is silent about firewall node for processing a packet based on modified address wherein one of the firewall node is selected from the cluster of firewall nodes within a single network.

Zenchelsky teaches one of the firewall nodes for processing a packet (see Abstract, figure 2, column 2, lines 52-67, column 3,lines 21-40);receiving and reading, the received packet (see Abstract, figure 2-3, column 2, lines 52-67, column 3,lines 21-40);a modified address based on the N-tuple space assigned to the first processing unit, such that the modified address does not conflict with addresses assigned by any of the other plurality of processing units and sending the packet based on the modified N-tuple address (see Abstract, figures 5a-5b, column 2, lines 52-67, column 3,lines 21-67, for assigning different IP address from IP pool and/or updating the user IP address each time user access authenticated, see column 8, lines 1-36 and figure 8A -8C for packet transmission based on peer-in / peer- out hash table based on rule identifier).

Bommareddy teaches a firewall cluster within the single network (see figures 1, 4, and 8, column 1, line 66 – column 2, line 60, column 3, line 1 – column 4, line 58, column 6, line 13 – column 8, line 45, column 9, line 5 - column 10, line 67) and processing the set of data packet from first packet from first address to second address wherein the second address being within a range of addresses assigned by firewall cluster ((see figures 1, 4, and 8, column 1, line 66 – column 2, line 60, column 3, line 1 – column 4, line 58, column 6, line 13 – column 8, line 45, column 9, line 5 - column 10, line 67, column 11, lines 9-65, column, column 15, line 40 – column 18, line 36)).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the teachings of Bosley, Zenchelsky and Bommareddy to provide a enhanced packet switched data handling method to a high speed network device securely switching data between the high speed network devices communicating behind the firewall clustering system using a enhanced hash function and arithmetic operations whereas the firewall cluster system being configured to operate in manner that creates or configures a firewall cluster on both internal and external network flow controllers to monitor the health of firewalls by probing firewall data packets through both internal and external firewalls whereas the flow controllers distribute traffic based on the source and destination IP addresses of a packet and ensuring that all IP-based protocols are supported and within the range of IP based protocols and repeating the same method steps until all data packets has been processed or securely transmitted to the destination port.

AS per claim 11, Zenchelsky teaches reading as the N-tuple address, a plurality of values from the received packet.(see Abstract, figures 5a-5b, column 2, lines 52-67, column 3,lines 21-67, see column 8, lines 1-36 and figure 8A -8C for packet transmission based on peer-in / peer- out hash table based on rule identifier).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the teachings of Bosley, Zenchelsky and Bommareddy to provide a enhanced packet switched data handling method to a high speed network device securely switching data between the high speed network devices communicating behind the firewall clustering system using a enhanced hash function

and arithmetic operations whereas the firewall cluster system being configured to operate in manner that creates or configures a firewall cluster on both internal and external network flow controllers to monitor the health of firewalls by probing firewall data packets through both internal and external firewalls whereas the flow controllers distribute traffic based on the source and destination IP addresses of a packet and ensuring that all IP-based protocols are supported and within the range of IP based protocols and repeating the same method steps until all data packets has been processed or securely transmitted to the destination port.

As per claim 12, Zenchelsky teaches reading at least a source port. (see Abstract, see column 1, lines 27-65).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the teachings of Bosley, Zenchelsky and Bommareddy to provide a enhanced packet switched data handling method to a high speed network device securely switching data between the high speed network devices communicating behind the firewall clustering system using a enhanced hash function and arithmetic operations whereas the firewall cluster system being configured to operate in manner that creates or configures a firewall cluster on both internal and external network flow controllers to monitor the health of firewalls by probing firewall data packets through both internal and external firewalls whereas the flow controllers distribute traffic based on the source and destination IP addresses of a packet and ensuring that all IP-based protocols are supported and within the range of IP based

protocols and repeating the same method steps until all data packets has been processed or securely transmitted to the destination port.

13. - 15. (Cancelled).

As per claim 16, Bosley discloses determining the quadrant identifier value based on a hash function and a modulo division [hash value based on number of bit of that represented as hypercube, the person skill in the art would recognize such hash value generation based on hash function and a modulo division, see figures 2-6, column 6, line 30- column 7, line 50, see column 9, lines 4-24].

As per claim 17, Bosley discloses adding a value to the N-tuple address, such that the modified N-tuple address is within the N-tuple space assigned to the first processing unit (see column 12, lines 12-41, adding node based on hash).

18. - 20. (Cancelled).

As per claim 21, Bosley discloses using a computer as the first processing unit (see Figure 1, column 5, lines 11-21).

As per claim 22, Bosley discloses routing using a router as the first processing unit (see column 4, line 40- column 5, line 53, routing).

23. (Cancelled).

As per claims 1-7, 27-28, and 30-36, claims 1-7, 27-28, and 30-36 are system claims of method claims 10-18. They do not teach or further define the limitation as recited in claims 10-18. Therefore, claims 1-7, 27-28, and 30-36 are rejected under same rationale as discussed in claims 10—18, supra.

As per claims 24-26, claims 24-26 do not teach or further define the limitation as recited in claims 10-18. Therefore, claims 24-26 are rejected under same rationale as discussed in claims 10—18, supra.

As per claims 29 and 37, claims 29 and 37 are firewall cluster claims of method claims 10-18. They do not teach or further define the limitation as recited in claims 10-18. Therefore, claims 29 and 37are rejected under same rationale as discussed in claims 10—18, supra.

As per claims 38-45, claims 38-45 are computer readable storage medium claims of method claims 10-18. They do not teach or further define the limitation as recited in claims 10-18. Therefore, claims 38-45 are rejected under same rationale as discussed in claims 10—18, supra.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See accompanying PTO 892 form.

a. System and method for detecting and countering a network attack by Etheridge et al. US Publication Number 2004/0054925 A1.

b. Hash-based systems and methods for detecting, preventing, and tracing network worms and viruses by Milliken US Publication Number 2003/0115485 A1.

c. Dynamic packet filter utilizing session tracking by Goldberg et al. US Publication Number 2004/0013112 A1.

d. IP datagram over multiple queue pairs by Graham et al. US Patent Number 7,133,405 B2.

e. Handling packet fragments in a distributed network service environment by Albert et al. US Patent Number 6,742,045 B1.

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Contact Information

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Saket K. Daftuar whose telephone number is 571-272-8363. The examiner can normally be reached on 8:30am-5:00pm M-W.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Follansbee can be reached on 571-272-3964. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Saket K Daftuar/

Examiner, Art Unit 2451

/John Follansbee/

Supervisory Patent Examiner, Art Unit 2451